УДК 344.633:004

СИСТЕМА CARD2CARD В МЕХАНИЗМЕ ХИЩЕНИЙ ПОСРЕДСТВОМ СЕТИ ИНТЕРНЕТ

Д. С. Захаров
курсант 3 курса факультета милиции
Могилевского института МВД (Беларусь),
32 взвод
Научный руководитель: ***Д. И. Шнейдерова****,*
преподаватель кафедры правовых дисциплин
Могилевского института МВД (Беларусь)

Согласно статистическим данным МВД Республики Беларусь, число киберпреступлений с каждым годом увеличивается в 2 и более раза: 2018 г. — 4741, 2019 г. — 10539, 2020 г. — 20575 преступлений [1]. При этом 90 % из указанных данных составляют хищения с банковских карт, реализуемые через сеть Интернет. Процент раскрываемости таких преступлений достаточно низкий, что связано с трудностями получения оперативной информации ввиду осуществления преступных действий с использованием VPN-серверов, изменяющих IP-адреса устройств.

Развитие информационных технологий позволило внедрить новый способ осуществления денежных переводов между банковскими и виртуальными картами без посещения отделений банка или почты. Такая система получила название Card2Card. Ее суть заключается в упрощенной процедуре денежных переводов между картами с использованием сети Интернет, реализация может осуществляться через программное обеспечение на компьютере или приложение на мобильном устройстве. Для проведения операции достаточно знания реквизитов входящей и исходящей карт, при этом не все приложения, поддерживающие такую систему, требуют процедуры регистрации, что позволяет осуществлять операции анонимно. Данное преимущество привлекло внимание киберпреступников, использующих указанные сервисы в качестве средства реализации преступных намерений или вывода и сокрытия похищенных средств на онлайн-кошельки.

Система Card2Card в качестве средства хищения применяется в случае, когда пользователи, используя сервис, вводят данные своих банковских карт, откуда в последующем преступниками списываются имеющиеся средства и переводятся не по заданному назначению, а на онлайн-кошельки киберзлоумышленников. В случае, когда система используется для вывода средств и сокрытия похищенного, первоначально преступниками реализуется сам механизм хищения, где данные карт получаются благодаря фишинговым сайтам, базам дан-

ных, купленным в сети DarkNet, либо вишингу, успешно минуя программу защиты 3-D Secure, применяемую банками для интернет-платежей.

Таким образом, ненадежность и низкий уровень защиты данных позволили активно использовать сервис Card2Card в механизме хищений посредством сети Интернет, что является актуальным вопросом для правоохранительных органов в борьбе с киберпреступностью.

---

1. Профилактика киберпреступлений [Электронный ресурс] // Официальный сайт УВД Могилевского облисполкома [сайт]. URL: https://mogilev.mvd.gov.by/ru/news/2566 (дата обращения: 04.02.2021). Перейти к источнику Вернуться к статье